ePDQ

User Guide – Risk & Fraud

V5.0 Released March 2009

Software Version: 5.9 Payment Engine & Internet Authentication

COPYRIGHT NOTICE
No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means electronic or mechanical, including photocopying and recording, for any purpose, without the prior written permission of Product Development, Barclaycard Payment Acceptance, Barclays Bank PLC.

Section	Topic	Products
D Risk & Fraud	**Risk Management**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 6 Page 109 Risk Manager Guide 5.9.

As well as core transaction processing, ePDQ provides a very comprehensive Risk Management module. This provides standard rules, lists and default checks that can be used to try and identify and alert you to potentially fraudulent transactions.

Risk Management systems such as that offered by ePDQ, can help you to recognise and hopefully remove fraudulent transactions from being processed through your business.

No Risk Management system can definitively determine whether any given transaction is, in fact, fraudulent. Therefore, fraud protection systems can form only one part of a comprehensive business decision-making process that involves human oversight and investigation of each transaction in question.

The responsibility to instill such a review process lies with your general business policies on risk and not with the Barclaycard Business ePDQ product.

The information in this section provides you with instructions on how you may wish to implement strategy rules. You must ensure that you periodically review which risk management tools are effective for your business and should ensure you understand what volume of transactions are being rejected by your strategy rules.

This section details the most common risk management tools adopted and provides examples of strategy rules, lists and velocity checks that you may wish to use.

IMPORTANT! All strategy rules examples are provided in good faith to enhance your understanding of how to effectively use the Risk Management features of ePDQ. We are unable to test these strategy rules for each individual application and therefore recommend that you set the action on any new strategy rules to "Review" to ensure they meet your business requirements.

By default all Strategy rules are INACTIVE. You must choose which rules to activate.

If activated, you should then manually accept or reject the transaction. If the fraud rule is not triggered when you believe it should be, please contact us immediately. You use all strategy rules at your own risk. Barclaycard Business does not accept liability for any losses incurred as a result of any fraud rule(s) activating incorrectly, failing to activate or operating in an unanticipated manner.

Section	Topic	Products
D Risk & Fraud	**Familiarising yourself with Strategy rules**	CPI MPI Lite

Main Document Reference	Risk Manager Guide, Chapter 3 Page 31

ePDQ provides a set of standard strategy rules. A full list can be obtained within the main Risk Manager Guide on page 28. When working with strategy rules, it is important that you understand how they work, and how to create new rules to suit your business.

To view the strategy rules:

1. After you have logged into the store, click **Risk Management** from the top four options.
2. Select **Rules** from the **Settings** menu on the left. The **Where are my Strategy Rules?** page is displayed.
3. Select **Click here to view My Rules** The standard set of strategy rules are displayed

TIP! By default, all of the strategy rules are inactive. You have to manually activate a fraud rule before it will function.

You can view the details of what the rule does by clicking on the relevant **Rule Name**. This displays the **My Rules Editor** page and shows the template screen for all new rules. The rule editor page displays the various components of the rule. These are:

- **Rule Name.** Either the standard or bespoke name assigned to a rule. If you create your own names you should ensure they are meaningful and relevant.
- **Description.** If you create your own description you should ensure it is meaningful and relevant.
- **Active Rule.** The option to activate the rule. This must be selected for the rule to function.
- **Process Code.** This determines whether the rule will be invoked before or after ePDQ attempts authorisation. Set to **Pre-Process** for before, or **Post-Process** for after. Some rules (such as AVS) can only be Post-Process.
- **Rule Weight.** Assign a numeric weight to the rule to control the impact a rule has on determining if a transaction is fraudulent. Further information on Weights can be found in the Risk Manager Guide "Using Rule Weighting" on page 128.
- **Rule Expression.** This shows the parameters of the rule being applied. You can write an expression directly into the expression box, or you can build an expression using the Attribute, Operator and Value fields.
- **Attribute.** This is the parameter that the fraud rule looks for to apply its checks, such as Card Number or Billing Name.
- **Operator.** Defines how you wish to treat the attribute (i.e. "equals", ""greater than", "does not equal").

- **Free Form Value.** Allows you to enter a specific value for the rule to look for. For example, if the Attribute you select is Billing Name, the value could be "John Smith".
- **Calculated Value.** Defines a value such as current month, in which the engine calculates which month the transaction is being evaluated in. Further information on Calculated Values can be found in the Risk Manager Guide on page 48.
- **Action.** Applies an action to rule if the transaction criteria meets the rule parameters. If the rule is triggered, the options are:
    - **Accept.** Allows the transaction to be processed.
    - **Reject.** Will stop the transaction being processed and will return a declined response to the cardholder.
    - **Review.** Holds the transaction in a pending state until you manually either accept or reject the transaction.
    - **Notify.** Lets you know via email that a transaction has triggered a fraud rule but does not interrupt transaction processing.
    - **Trace.** Lets you know via an API message that a transaction has triggered a fraud rule but does not interrupt transaction processing. This is only valid for ePDQ MPI users.
- **Action on Missing Value.** This can be applied if you wish to trigger a rule because a cardholder fails to submit a value (for example, email address). The actions associated are the same as above.
- **Rule Auto Actions.** This can be applied if you want the rule to add values to one or more block/accept lists. Further information on **Rule Auto Actions** can be found in the Risk Manager Guide, for instructions on how to create rules that add values to a list, see page 79.
- **Merchant Message.** This is displayed in the Store Admin should the transaction be identified by a fraud rule.
- **Storefront Message.** This can only be used if you use the ePDQ MPI product.
- **Send e- mail notification to.** Allows you to specify an additional email address for the merchant message to be sent. This could be sent to your admin team, or to a specific fraud team.

Each of the standard strategy rules have all of the above configured. It may be beneficial to review some of the standard rules to familiarise yourself with how each parameter can be configured.

When you initially start to use strategy rules we would recommend that you only activate two or three and monitor the impact they are having on your transaction processing. It may also be prudent to adjust the **Action** on any active strategy rules to **Notify** so that you can monitor levels of transactions triggering strategy rules without impacting customers.

TIP! If you have regular customers that you do not wish to be checked by strategy rules, you can create a new rule and set the Attribute to be their card number or name, and then set the Action to "Accept". If you put this as the first rule in the sequence their transaction will not be checked by any other strategy rules.

Section	Topic	Products
D Risk & Fraud	**Adding a New Fraud Rule**	CPI MPI Lite

Main Document Reference	Risk Manager Guide, Chapter 5 Page 39

You can create new rules, specific to your business, or can create different variations of the standard rule suite. The examples below show how to create new rules to:

- Review transactions submitted with a delivery country of UK.
- Accept all transactions from cardholder John Smith from Northampton.
- Reject any transactions that have a CV2 result of "not matched".

All new strategy rules are created from the My Rules Strategy page. To access this:

1. After you have logged into the store, click **Risk Management** from the top four options.
2. Select **Rules** from the **Settings** menu on the left. The **Where are my fraud rules?** page is displayed.
3. Select **Click here** to view your rules. The standard set of strategy rules is displayed.
4. Scroll down to the bottom and select **Add**. A **My Rules New Rule** page will be displayed with a blank template **New Rule**.

Example 1 - Review transactions submitted with a delivery country of UK.

1. On the **New Rule** page enter the **Rule Name.** For this example enter "Block UK Delivery".
2. Select the Active flag
3. Select the **Process Phase** of **Pre-Process** as we wish the transaction to be checked before ePDQ obtains authorisation.
4. Select the **Attribute** of **Order Form Lists** and **ShipToCountry**.
5. Select the **Operator** of **=(Equal To or In).**
6. Select **Free Form Value** and enter the three digit country code into the **Value** field. For UK this would 826. A full list of country codes is provided in the Store Admin Guide in Appendix D.
7. Click the **Add to Expression** button. The expression you have just built will be entered into the expression box.
8. Set the **Action** to **Review**. This will mean that if any transactions meet this criteria, they will be flagged as potentially fraudulent and will be placed in a review queue.
9. Set the **Action On Missing Value** to **Review** as well. This means that if the cardholder fails to enter any delivery country, the transaction will be marked for review. Please remember that this will apply to any country, not just the UK.

10. Create a Merchant and Consumer Message as appropriate.
11. If you wish to receive an additional email advising that this rule has been triggered, enter an email in **Send notification email to** field.
12. If you are happy with the details you have entered, then press **Save** at the bottom of the page. The rule will now be active.

With any new rule, its sequence number is set to be the last rule checked. You can change the sequence number by overwriting a new value in the **Seq #** field.

Example 2 - Accept all transactions from cardholder John Smith from Northampton.

1. Ensure that you have opened up a new blank template rule.
2. On the **New Rule** page enter the **Rule Name.** For this example enter "Accept John Smith".
3. Select the **Active** flag
4. Select the **Process Phase** of **Pre-Process** as we wish the transaction to be checked before ePDQ obtains authorisation and before any other rules are checked.
5. Select the **Attribute** of **Order Form Lists** and **BillToName**.
6. Select the **Operator** of **=(Equal To or In).**
7. Select **Free Form Value** and enter the **Value** of John Smith. The Value is case sensitive so would not pick up john smith.
8. Click the **Add to Expression** button. The expression you have just built will be entered into the expression box.

   As you are checking two attributes (name and town), you have to enter the second attribute.

9. Click **AND (&)** to add a second attribute. This will mean that the transaction will look for details that contain John Smith AND Northampton.
10. Select the **Attribute** of **Order Form Lists and BillToCity**.
11. Select the **Operator** of **=(Equal To or In).**
12. Enter the **Value** of Northampton.
13. Click the **Add to Expression** button. The additional expression you have just built will be entered into the expression box.
14. Set the **Action** to **Accept.** You can leave the **Action On Missing Value** blank as you are looking for specific details.
15. Create a Merchant and Storefront Consumer as appropriate.
16. If you are happy with the details you have entered, then press **Save** at the bottom of the page. The rule will now be active.

The rule will now be listed with the other standard rules. You should change the **Seq #** to 1, so that this rule is checked first and will allow John Smith from Northampton to go straight for authorisation without any further checks.

To change the sequence, overwrite the existing number with the new sequence number and click in a clear space on the page. The new order will be displayed.

Example 3 - Reject any transactions that have a CV2 result of "not checked".

The standard CV2 rule is only triggered when the response is "Not Matched". This delivers a "Cvv2Response code" of "2". If any other response is returned the rule would not be triggered.

You may wish to support your risk policy by also checking transactions where the CV2 result was anything other than "Not Matched"

1. Ensure that you have opened up a new blank template rule.
2. On the **New Rule** page enter the **Rule Name.** For this example enter "Block CV2 Not Checked".
3. Select the **Active** flag
4. Select the **Process Phase** of **Post-Process** as this rule has to check the CV2 result returned from the card issuer.
5. Select **Attribute of Order Form Fields** and **Cvv2Response.**
6. Select **Operator** of **=(Equal To or In).**
7. Enter **Value** of **3.** For a list of possible values, see the Risk Manager Guide, page 244-245.
8. Click the **Add to Expression** button.

   TIP! You could broaden the range of not checked responses by selecting "OR" within the expression builder, and then adding further attributes, such as 5, 6 or 7. You will need to Click the Add to Expression button after you change each value. The expression would be:

   {Cvv2Response} = "3" | {Cvv2Response} = "5" | {Cvv2Response} = "6" | {Cvv2Response} = "7"

9. Set the **Action** to **Reject.** This means that any transaction that is returned with any of the CVV2 responses above will be rejected as potential fraud.
10. Create a Merchant and Consumer Message as appropriate.
11. If you are happy with the details you have entered, then press **Save** at the bottom of the page. The rule will now be active.

The rule will be placed at the bottom of the standard rule sequence. Change the sequence number if you wish this rule to be activated earlier in the rule order.

Section	Topic	Products
D Risk & Fraud	**Finding Fraudulent Transactions**	CPI MPI Lite

Main Document Reference	Risk Manager Guide, Chapter 10 Page 153

Whenever a strategy rule is triggered that identifies a transaction as potentially fraudulent the details are added to a list. You can view this list to identify the level of transactions being processed through your store that trigger your strategy rules.

1. After you have logged into the store, click **Risk Management** from the top four options.
2. Under the **Transactions** menu on the left, you have two options:

   - **Fraudulent.** This will provide a search screen allowing you to search for transactions that have been marked as fraudulent. Enter your search criteria and click search to see a list of fraudulent orders.

     You can display:

     - **All** transactions which will return all transactions that have been marked for review.
     - **Review.** Those transactions that have to be reviewed and either accepted or rejected.
     - **Accepted.** Transactions that have already been reviewed and have been accepted.
     - **Rejected.** Transactions that have already been reviewed and have been rejected.
     - **Voided.** Transactions that have already been reviewed and have been void.
     - **Chargeback.** This will provide a search screen that allows you to search for all transactions that you have marked as receiving a chargeback.

   - **Review.** With each fraud rule, you can set the action to Accept, Reject, Review, Notify or Alert. This option will provide a list of all transactions that have been marked for review. For each transaction you will have an "Approve" or "Reject" option.

     Reviewing transactions is a manual process and will require you to make a decision on whether to approve or reject the transaction. This decision may be based on additional information you have gained from the cardholder (i.e. the cardholder may have provided you with additional security information).

Section	Topic	Products
D Risk & Fraud	**Reviewing Fraudulent Transactions**	CPI MPI Lite

Main Document Reference	Risk Manager Guide, Chapter 10 Page 153

If you have the **Action** on any strategy rules set to **Review** then these transactions require further action to be completed. The transactions falling into this category can be viewed by following the instructions in the last section.

When dealing with transactions in review state you must be clear on what type of transaction they are, as the process is different for PreAuth and Auth transactions.

- **PreAuth** transactions that you approve must also be marked as shipped. Simply selecting "Approve" will not place the transaction in the settlement batch. If you do approve the transaction, you should then follow the instructions shown in "Marking a Transaction Shipped" in Section B.
- **Auth** transactions will automatically be placed in the settlement batch once you approve them.

To review a transaction:

1. After you have logged into the store, click **Risk Management** from the top four options.
2. Under the **Transactions** menu on the left, select **Review.** A list of all transactions requiring review will be displayed. Each transaction will have an **Approve** or **Reject** check box.
3. If you wish to see which fraud rule was triggered by this transaction, click the **Order ID**. This will display the **Order Detail Page.** If you then click on the **Transaction ID** that is marked as fraud, the **Fraud Rule ID** will be displayed.
4. Once you have identified which transaction you wish to review, select either the **Approve** or **Reject** check box.
5. Click **Set Review Status** under the **Operations** menu on the left.
6. A **Transaction Management** page will be displayed confirming your action.

You must ensure that if the transaction was a **PreAuth** transaction type that you also mark it for shipment. Failure to do this will result in the transaction not being settled.

Section	Topic	Products
D Risk & Fraud	Recording Chargebacks	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 5 Page 97

You may at some stage, be charged back for a transaction. This means that you will be required to pay back the money for the transaction to the card issuer. Whilst you can use some of the techniques offered by ePDQ to limit the number of chargebacks you receive, you may not be able to avoid them completely.

It is very important to record when a chargeback has been received. By doing this, ePDQ automatically records the card number used and adds it to a Block list. This way, if the card is presented again, it will be declined or put into a review state if you are using the strategy rules.

To record a chargeback, you first have to locate the transaction in ePDQ, an order must be settled in order for it to be recorded as a chargeback. This can be done by searching for the transaction by the cardnumber, or by the date and time. Follow the instructions in "Finding and Order by Order ID" and instead of searching by order ID, search by card number and date.

Once you have located the transaction, you should check it is the correct order, and then follow the instructions below:

1. Click the **Order ID** of the order. The **Order Detail Page** is displayed.
2. An option of **Chargeback** is available under the **Operations** menu on the left. Click **Chargeback** to display the **Chargeback Management** page.
3. Select the box to the left of the transaction you want to record as a chargeback.
4. Select the reason for the chargeback (as displayed on your chargeback letter).
5. Click **Submit Chargeback** from the menu on the left. The transaction has now been marked as a chargeback. A **Transaction Management Response** page will be displayed.

TIP! You must activate the block cardnumber fraud rule to ensure that any transactions marked as chargebacks are added to the block card list and checked each time. This will ensure the same card number is not accepted again.

TIP! If you have more than one ePDQ store, you will have to manually add any cards you wish to block to each store.

Section	Topic	Products
D Risk & Fraud	**Address Verification Service (AVS)**	CPI MPI Lite

Main Document Reference	Risk Manager Guide Appendix 8 Page 243

Address Verification is a UK based service that checks the details supplied for the cardholders billing address and post code against that held on the Card Issuers records. ePDQ simply passes the address information and receive the AVS response from the issuer. We are not responsible for the values returned.

Two components of the address are checked; the numerics of the house number and the numerics of the postcode. For example, if 1 High Street, NN4 7SG was the address, ePDQ would submit "1, 4, 7". The card issuer would then check these details and return a response based on what values match. The potential results returned are:

Response Code	AVS Display	Description
S1	(Blank)	AVS not checked (see TIP)
B1	YN	Post code not checked; address match,
B2	NN	Post code not checked; address no match
B3	NN	Post code not checked; address partial match
B4	NY	Post code match; address not checked
EX	YY	Address and Post code match
B5	NY	Post code match; address no match
B6	NY	Post code match; address partial match
B7	NN	Post code no match; address not checked
B8	YN	Post code no match; address match
N	NN	None match
B9	NN	Post code no match; address partial match
BA	NN	Post code partial match; address not checked
BB	YN	Post code partial match; address match
BC	NN	Post code partial match; address no match
BD	NN	Post code partial match; address partial match
7	UU	Response not valid (see TIP)

There are two standard AVS rules. These are only triggered for a non match:

- AVS Address Does Not Match. Triggered on NY or NN.
- AVS Zip Does Not Match. Triggered on YN or NN.

TIP! The standard rules will not be triggered for AVS not checked (Blank/S1) or Response not valid (UU/7). You may wish to set up a separate fraud rule to capture and act on these responses. See the next Topic for more information.

Section	Topic	Products
D Risk & Fraud	**Adding Additional AVS Rules**	CPI MPI Lite

Main Document Reference	Risk Manager Guide Appendix B Page 243

The standard AVS rules are only triggered if the AVS result is returned as failed, and uses the generic "Y" and "N". This leads to very general checking as there are only four responses (YY, YN, NY and NN). You can create additional strategy rules that use the more detailed **Response Codes** shown on the last page to create more bespoke AVS checking and to block orders at a more detailed level.

The example below is based on a fraud rule where you only wish to reject any transactions that completely failed the post code match and only had a partial address match.

1. Ensure that you have opened up a new blank template rule.
2. On the **New Rule** page enter the **Rule Name.** For this example enter "BlockAVSRule1".
3. Select the **Active** flag
4. Select the **Process Phase** of **Post-Process** as this rule has to check the AVS result returned from the card issuer.
5. Select **Attribute Order Form Lists** and **AVSResponseCode.**
6. Select **Operator** of **=(Equal To or In).**
7. Enter **Value** of **B9.**
8. Click the **Add to Expression** button. The expression will be added to the expression box.
9. Set the **Action** to **Reject**. This means that any transaction that is returned with the specific AVS Response above will be rejected as potential fraud.
10. Create a Merchant and Consumer Message as appropriate.
11. If you are happy with the details you have entered, then press **Save** at the bottom of the page. The rule will now be active.

If you only wish to use your bespoke AVS rules, you should ensure that no others are activated.

As with other examples in this section, you can add multiple attributes using the '**AND**' or '**OR**' options.

Section	Topic	Products
D Risk & Fraud	**Card Security Code (CSC) (CV2)**	CPI MPI Lite

Main Document Reference	Risk Manager Guide Appendix B Page 244

The Card Security Code is the unique 3 digit code on the rear of most cards, and 4 digit code on the front of American Express cards. It is used to identify that the cardholder has possession of the card at the time of purchase. The CSC is also referred to as CV2, Cvv2 and CVM. The table below displays the name displayed for results supplied.

The CSC data cannot be stored by you or us and must not be displayed on any receipt.

As with Address Verification, the CSC supplied is sent to the card issuer in the authorisation record. The card issuer will then check their records to confirm whether the submitted data matches. ePDQ simply passes the card security data and receive the CSC response from the issuer. We are not responsible for the values returned. The responses returned from the issuer could be:

CVM Response	CCE Response (ePDQ)	Description
2	1	CSC matches
4	2	CSC does not match issuer value
1	3	CSC was not processed
Unknown	6	CSC invalid or missing
X	7	No response from server

TIP! The default ePDQ Fraud Rule "CVV2 DoesNotMatch" will only be triggered by a CSC response of 2. No other response from an issuer will trigger the rule. You can however, set up your own rule to check for other responses.

1. Ensure that you have opened up a new blank template rule.
2. On the **New Rule** page enter a **Rule Name.**
3. Select the **Active** flag
4. Select the **Process Phase** of **Post-Process.**
5. Select **Attribute of Order Form Lists** and **Cvv2Response.**
6. Select **Operator** of **=(Equal To or In).**
7. Enter **Value** of **3. TIP! You can add further values to the expression (i.e. 6 & 7) to catch all.**
8. Click the **Add to Expression** button. The expression will be added to the expression box.
9. Set the **Action** to **Reject**. This means that any transaction that is returned with the specific CSC Response(s) above will be rejected as potential fraud.
10. Create a Merchant and Consumer Message as appropriate.
11. If you are happy with the details you have entered, then press **Save** at the bottom of the page. The rule will now be active.

Section	Topic	Products
D Risk & Fraud	**Points to remember for using AVS and CSC checks**	CPI MPI Lite

Main Document Reference	None

The information provided below is to help you understand the Address Verification and Card Security Code checks.

- The company that issued the card is responsible for performing the Card Security Code and Address checks. It will also provide you with verification responses. We will not be able to give advice concerning the reason for a particular decision.

- You should make sure that Card Security Code and Address verification information is never stored on file (i.e. we recommend that you do not pre-populate this data from a cardholder database as it may have changed.). Instead, this information should be obtained from the cardholder for each transaction. The service can be used for first or individual transactions, but not for recurring transactions using the same card details.

- It is your decision whether or not to proceed with the transaction after the response has been received from the company that issued the card. These extra checks have been designed to help you decide whether or not to proceed with the transaction. The card Security Code and Address Verification Service is not an absolute guarantee of payment, but a valuable additional check.

- You must activate the ePDQ strategy rules to allow ePDQ to take any action on responses received. Whilst, ePDQ will submit Card Security Code and Address Verification information, the responses will only be returned for information and presented in the Order Detail. To either Accept, Reject or Review transactions based on the AVS or CSC responses you must have activated the strategy rules.

- You must fully understand which responses will trigger the default rules. They will not be triggered by all possible responses returned by the issuer. Please see the previous topics for further information on what will trigger the rules.

- AVS and CSC checks are applicable for all currency types.

- AVS and CSC checks are applicable for UK issued cards only.

- AVS and CSC is supported on Visa, MasterCard and Maestro card types only.

Section	Topic	Products
D Risk & Fraud	**Fraud Rule Responses for the ePDQ CPI**	CPI

Main Document Reference	None

If you are using the ePDQ CPI, you will typically receive the responses of either success or declined.

You must be aware, however, that if you activate strategy rules, additional responses will be sent from the CPI to your web site. When integrating the CPI you must cater for this and should not restrict your web site to only handle success or decline messages.

Please ensure you have configured your Post URL script to handle the additional responses sent back to your site once a fraud rule has been activated.

For more information, refer to the CPI Integration Guide or contact your web developer.

Section	Topic	Products
D Risk & Fraud	Internet Authentication (Verified by Visa & SecureCode).	CPI MPI

Main Document Reference	Store Administrator Guide, Appendix B Page 167

Background

ePDQ CPI and MPI users can benefit from enhanced protection against chargebacks afforded by Internet Authentication services such as Verified by Visa for Visa cards and SecureCode for MasterCard and Maestro cards. ePDQ Lite merchants cannot use these services as it requires the cardholder to enter personal information on the payment page.

Authentication services require the cardholder to authenticate themselves by the use of a secure PIN or password at the point of purchase. This is achieved by your web site displaying a specific pop up box or page containing information supplied by the card issuer to authenticate their cardholder.

To participate in the service you must have registered with us. MPI users are required to have correctly integrated their Authentication software. CPI users require no additional integration but must instruct us that they wish to use these services.

How you may benefit

As described above, by asking the cardholder to authenticate their identity the likelihood for fraud is greatly reduced. A fraudster will be unable to simply enter a card number to fraudulently obtain goods and services. Anybody attempting to use a card that does not belong to them will have to know the authentication information.

Even if the card is not enrolled in the Authentication services, you as a merchant can still benefit from 'attempted authentication'. It is important that you read and understand our Internet Authentication Procedure Guide to identify when this is possible.

Whilst Verified by Visa and SecureCode authenticates the cardholder, you must still check the card. This is done using the standard authorisation process. It is at this stage that the other risk management rules can be applied. An example of this is where a cardholder correctly authenticates themselves but has provided an address that you will not deliver to – in this scenario despite authentication being successful, the transaction may be declined or marked for review.

IMPORTANT – Internet Authentication is an additional tool to help reduce fraud. You must also use the risk management tools provided to further reduce your risk. We advise against using Internet Authentication as your only means of fraud protection

Section	Topic	Products
D Risk & Fraud	**Authentication Results**	CPI MPI

Main Document Reference	Store Administrator Guide Appendix B Page 167

If you have signed up for ePDQ and have activated the authentication software, you will receive an authentication response for each Visa, MasterCard or Maestro transaction processed through your web site.

Depending on the liability shift available (as detailed in the Internet Authentication Procedure Guide, which will be provided when you sign up for the service), you will be afforded protection against certain chargebacks.

The results returned by ePDQ for authentication transactions are:

Payer Security Level Value	Message	What this means.
0	Authentication is not supported.	No liability shift.
1	Authentication is supported, but the cardholder is not enrolled.	Attempted liability shift subject to scheme rules.
2	Authentication supported. Authentication succeeded.	Liability shift subject to scheme rules.
3	Authentication supported. Authentication failed.	Visa – the transaction will be declined. MasterCard and Maestro – if transaction authorised by Card Issuer no liability shift.
4	Authentication supported but authentication results unavailable.	No liability shift.
5	Authentication supported, BIN not in range.	Attempted liability shift subject to scheme rules.
6	Attempted to enroll the cardholder in a payer authentication system, but the attempt was not successful.	Attempted liability shift subject to scheme rules. For Visa, an IAV should also be returned.

Visa, MasterCard and Maestro support an Issuer Authentication Value (IAV) to determine the result of an authentication response. This will be a unique value and will be displayed in the **PayerAuthenticationCode** field.

Some transactions will also have a unique transaction ID. This is used as an additional check as to the authentication history. This is displayed in the **PayerTxnID** field.

Section	Topic	Products
D Risk & Fraud	**Viewing Authentication Results**	CPI MPI

Main Document Reference	Store Administrator Guide, Appendix B Page 167 & 168

When you are processing transactions for authentication, you may need to know whether or not you have liability shift protection before fulfilling an order.

This topic shows how you can view the results of authentication for a transaction.

1. After you have logged into the store, click **Orders** from the top four options.
2. If the transaction was processed within the last 7 days, select **Recent Activity.** If you are unsure when the order was processed, select **Orders** from the menu on the left and enter your search criteria (see "Finding an Order by Order ID" for more information).
3. Once you have located the order you wish to view click the **Order ID.** This will open up the **Order Detail** page. Within the Order Detail, will be a list of totals and a sub total, **Transaction Detail** and **Billing Information.**
4. Click the **Transaction ID** within the **Transaction Detail** section. The **Transaction Detail** page is displayed.
5. You need to scroll down to **Processor Details** to view the authentication results. The key results you are looking for are:
   - **Payer Authentication Code.** This can be a value up to 64 characters and is the Issuer Authentication Value. (Known as CAVV for Visa and AAV for MasterCard and Maestro).
   - **Payer Security Level.** This will be one of the values as detailed in the previous topic.

   There may also be other results returned. For users of the Barclaycard Business Hosted Authentication Service, this value will typically be N/A as this check is performed by the hosted solution and not by the ePDQ payment engine.

   - **Payer Authentication Result Code.** This provides details of whether the Issuer Authentication Value was generated and processed correctly. A list of codes is provided on page 167 of the Store Administrator Guide.

6. Once you have viewed the results you need, you should go back to the main orders page to find further orders.

Section	Topic	Products
D Risk & Fraud	**Setting Strategy rules for Authentication**	CPI MPI

Main Document Reference	None

Typically, authentication results are maintained as information for a particular order. By default there are no standard strategy rules activated to look for authentication results. This is typically because most transactions subject to fraudulent activity may be covered either by full or attempted authentication liability shift.

You may however wish to set up a fraud rule that is triggered when an authentication response is negative (either not received, or the card issuer may advise that the cardholder could not successfully authenticate themselves.

IMPORTANT! Before adding any rule based on authentication you must first ensure that you understand that you may impact a transaction that has been authorised.

1. After you have logged into the store, click **Risk Management** from the top four options.
2. Select **Rules** from the **Settings** menu on the left. The '**Where are my fraud rules?**' page is displayed.
3. Select **Click here to view My rules.** The standard set of strategy rules is displayed.
4. Scroll down to the bottom and press **Add.** A **My Rules New Rules** page will be displayed with a blank template fraud rule.
5. On the New **Rule** page enter the **Rule Name.**
6. Select the **Active** flag
7. Select the **Process Phase** of **Pre-Process** and the **Action** (see point 10 below) to Reject if you wish to discontinue with the transaction or **Post Process** if you wish to evaluate the transaction based on the authentication and authorisation response.
8. Select **Attribute of Order Form Fields** and **PayerSecurityLevel**.
9. Select the **Operator** of **=(Equal To or In).**
10. Enter the code that you wish to trigger the rule. For a failed authentication, select **3**.
11. Click the **Add to Expression** button. The expression you have just built will be entered into the expression box.
12. Set the **Action** to whatever you wish to do with the transaction.
13. Leave **Action On Missing Value** as none.
14. Create a Merchant and Consumer Message as appropriate.
15. If you wish to receive an additional email advising that this rule has been triggered, enter an email in **Send notification email to** field.
16. If you are happy with the details you have entered, then press **Save** at the bottom of the page. The rule will now be active.

By activating this rule, any transaction that returns a Payer Security Level result of 3 will trigger the rule.

Section	Topic	Products
D Risk & Fraud	**Velocity Checks**	CPI MPI Lite

Main Document Reference	Risk Manager Guide, Chapter 8 Page 103

Velocity Checking introduces the ability to track and count transactions processed through your store and apply specific attribute checks (i.e. card number) and time/counter variables. The velocity checks should be used in conjunction with strategy rules to identify and block potentially fraudulent transactions. There are three types of velocity checks available.

- Counter-Based, Constant Velocity Checks.

  These use either fixed single, or multiple attributes such as card number or billing name and count how many times the attribute(s) are submitted. You can then use a fraud rule to specify a time period in which to monitor the velocity.

- Counter-Based, Change Detection Velocity Checks.

  This enables a single or multiple fixed attribute(s) (i.e. BillToName & IP address) to be checked against a variable attribute (i.e. card number). This will track how many different card numbers have been used against the same IP and billing name, enabling identification of randomly generated card numbers.

- Value-based Velocity Checks

  The value of a specified attribute is totaled from each matching order. Value based checks can determine the total order amount that has been placed in multiple orders using a specified Attribute of card number.

To make use of a velocity you will have to incorporate a "built-in function" from the fraud rule expression builder. The built in function for Velocity Checks is "CheckVelocity".

You then create a new fraud rule that uses the velocity and specify what criteria you want to check to activate the rule. It is important to remember that the velocity checks simply count how many times a specific attribute or variable is submitted through the engine.

TIP! The Process Code you use (pre-process or post-process) will impact when the velocity is triggered. For pre-process rules the velocity will be triggered after one further transaction is processed. If you specify a "value" of 2, this will not be triggered until after 3 attempts.

Section	Topic	Products
D Risk & Fraud	**Velocity Check Examples**	CPI MPI Lite

Main Document Reference	Risk Manager Guide, Chapter 8 Page 106

This topic provides an example for each of the types of attributes. By default, ePDQ does not have any velocities pre-configured. You can set up to a maximum of 20 velocities per store.

1. After you have logged into the store, click **Risk Management** from the top four options.
2. Select **Velocities** from the **Settings** menu on the left.

   A message will be displayed stating that no velocities have been created. Click **Next** to create a new velocity. The **Risk Management Velocities** page will be displayed. The name and description can be created according to your requirements. The types are:
   - Counter-based, constant
   - Counter based, change detection
   - Value based

Example 1 – Counter-based, constant

This example uses the attribute of cardnumber. We are looking to reject any transaction where the same card number is used more than twice within 1 minute (60 seconds).

Step 1. Creating the Velocity

1. From the **Risk Management Velocities** page enter an appropriate name and description.
2. Select **Type** of **Counter-based, constant.**
3. Enter a retention time (in seconds). This is the duration that the engine will retain the attribute information. Leave the default for 1 day (86400 seconds).
4. Select a **Processing Phase** of **Pre-Processing** or **Post-Processing** depending on which attribute you are going to use (for example, if the attribute were AVS response, you would have to use Post-Processing).
5. You can activate the velocity rule by selecting **Yes.**

   TIP! Activating a velocity will have no affect on transaction processing until you link the velocity to a fraud rule that performs an action (Accept, Reject etc).

6. Select the **Attribute** of cardnumber and click **Add Velocity Attribute.**
7. Select **Save New Velocity.** The velocity will now display in the velocity list link.

Step 2. Linking the Velocity to a Fraud Rule.

Now that you have created a velocity you can link it to a new rule which will be triggered should the criteria you set match.

1. From within the **Risk Management** section, select **Rules** from the **Settings** menu on the left. The '**Where are my fraud rules?'** page is displayed.
2. Select **Click here to view My rules.** The standard set of strategy rules is displayed
3. Scroll down to the bottom and press **Add.** A **My Rules New Rules** page will be displayed with a blank template fraud rule.
4. On the New **Rule Editor** page enter the **Rule Name.**
5. Select the **Active** flag
6. Select the **Process Phase** as appropriate (for this example, it should be Pre-Process).
7. Select **Attribute of Built in Function** and **Check Velocity**.
8. Select an Operator. If you wished to trigger the rule if a cardnumber is entered more than twice in 5 minutes, you should specify **> (Greater Than).**
9. Enter a **Value.** If you wish to check for occurrences of the same card number more than twice, enter **2.** (Note: For pre-process transactions this will not be triggered until after 3 attempts).
10. Click **Add to Expression.** The expression will appear in the expression box with some blank spaces, as shown below:

    {CheckVelocity(0,"",0)} > "2"

11. You need to specify the store that the check applies to, the velocity check you wish to apply, and the time (in seconds) you wish to check within the (0,"",0) section. Using store 44, the Velocity name of "CardCheck" and a time of 60 seconds, the expression would become:

    {CheckVelocity(44,"CardCheck",60)} > "2"

12. Set the **Action.** For this example, you would set to Reject.
13. Leave **Action On Missing Value** as none.
14. Create a Merchant and Consumer Message as appropriate.
15. If you wish to receive an additional email advising that this rule has been triggered, enter an email in **Send notification email to** field.
1. If you are happy with the details you have entered, then press **Save** at the bottom of the page. The rule will now be active.

Example 2 – Counter-based, change-detection

This example uses the constant attribute of card number but introduces a change detection of BillToCity. This will reject any transaction where the same card number is used but the billing city is different more than 3 times in 2 minutes (120 seconds).

Step 1. Creating the Velocity

1. From the **Risk Management Velocities** page enter an appropriate name and description.
2. Select **Type** of **Counter-based, change-detection.**
3. Enter a retention time (in seconds). This is the duration that the engine will retain the attribute information. Leave the default for 1 day (86400 seconds).
4. Select a **Processing Phase** of **Pre-Processing** or **Post-Processing** depending on which attribute you are going to use.
5. You can activate the velocity rule by selecting **Yes.**
6. Select the **Constant Attribute** of card number and click **Add Velocity Attribute.**
7. Select the **Change-Detection Attribute** of BillToCity and click **Add Velocity Attribute.**
8. Select **Save New Velocity.** The velocity will now display in the velocity list link.

Step 2. Linking the Velocity to a Fraud Rule.

1. From within the **Risk Management** section, select **Rules** from the **Settings** menu on the left. The **'Where are my fraud rules?'** page is displayed.
2. Select **Click here to view My rules.** The standard set of strategy rules is displayed
3. Scroll down to the bottom and press **Add.** A **New Rule** page will be displayed with a blank template fraud rule.
4. On the **New Rule** page enter the **Rule Name.**
5. Select the **Process Phase** as appropriate (for this example, it should be Pre-Process).
6. Within the **Attribute** field, you will need to select the **Built in Function and Check Velocity**.
7. Select an Operator. As you wish to trigger the rule if the Billing City is entered more than three times in 2 minutes, you should specify **> (Greater Than).**
8. Enter a **Value.** As you wish to check for occurrences of the same Billing City more than three times, enter **3**. (Note: For pre-process transactions this will not be triggered until after 4 attempts).
9. Click **Add to Expression.** The expression will appear in the expression box with some blank spaces, as shown below:

   {CheckVelocity(0,"",0)} > "3"

10. You need to specify the store that the check applies to, the velocity check you wish to apply, and the time (in seconds) you wish to check within the (0,"",0) section. Using store 56, the Velocity name of "BillingCheck" and a time of 120 seconds, the expression would become:

{CheckVelocity(56,"BillingCheck",120)} > "3"

11. Set the **Action.** For this example, you would set to Reject.
12. Leave **Action On Missing Value** as none.
13. Create a Merchant and Consumer Message as appropriate.
14. If you wish to receive an additional email advising that this rule has been triggered, enter an email in **Send notification email to** field.
15. If you are happy with the details you have entered, select **Active Rule** at the top of the page and then press **Save** at the bottom of the page. The rule will now be active.

With this velocity and rule activated, the rule will be triggered if transactions are submitted where the same card number is used but the billing city changes more than three times in 2 minutes.

Example 3 – Value-based

This example uses the constant attribute of card number but introduces a value of Transaction Total (TransTotal). This can then be used to reject a card, if it has been used to generate more than a specified transaction total (e.g. £500) in the last 5 minutes (300 seconds).

Step 1. Creating the Velocity

1. From the **Risk Management Velocities** page enter an appropriate name and description.
2. Select **Type** of **Value-based.**
3. Enter a retention time (in seconds). This is the duration that the engine will retain the attribute information. Leave the default for 1 day (86400 seconds).
4. Select a **Processing Phase** of **Pre-Processing** or **Post-Processing** depending on which attribute you are going to use.
5. You can activate the velocity rule by selecting **Yes.**
6. Select the **Constant Attribute** of card number and click **Add Velocity Attribute.**
7. Select the **Value-based Attribute** of TransTotal and click **Add Velocity Attribute.**
8. Select **Save New Velocity.** The velocity will now display in the velocity list link.

Step 2. Linking the Velocity to a Fraud Rule.

1. From within the **Risk Management** section, select **Rules** from the **Settings** menu on the left. The '**Where are my fraud rules?'** page is displayed
2. Select **Click here to view My Rules,** the standard set of strategy rules are displayed.
3. Scroll down to the bottom and press **Add.** A **New Rule** page will be displayed with a blank template fraud rule.
4. On the **New Rule Editor** page enter the **Rule Name.**
5. Select the **Process Phase** as appropriate.
6. Within the **Attribute** field, you will need to select the **Built in Function and Check Velocity**.
7. Select an Operator. As you wish to trigger the rule if the transaction total is greater than £500 **> (Greater Than).**
8. Enter a **Value.** As you wish to check for transaction total greater than £500 enter **500**.
9. Click **Add to Expression.** The expression will appear in the expression box with some blank spaces, as shown below:

   {CheckVelocity(0,"",0)} > "500"

10. You need to specify the store that the check applies to, the velocity check you wish to apply, and the time (in seconds) you wish to check within the (0,"",0) section. Using store 78, the Velocity name of "TransTotal" and a time of 300 seconds, the expression would become:

    {CheckVelocity(78,"TransTotal",300)} > "500"

11. Set the **Action.** For this example, you would set to Reject.
12. Leave **Action On Missing Value** as none.
13. Create a Merchant and Consumer Message as appropriate.
14. If you wish to receive an additional email advising that this rule has been triggered, enter an email in **Send notification email to** field.
15. If you are happy with the details you have entered, select **Active Rule** at the top of the page and then press **Save** at the bottom of the page. The rule will now be active.

With this velocity and rule activated, the rule will be triggered if transactions are submitted where the same card number and the transaction total of one, or many transactions within 300 seconds exceeds £500.

You can apply multiple constant attributes (i.e. card number and email address) and multiple change detection attribute (i.e. billing name, IP address) to try and pinpoint potential fraud. A list of the velocity checks attributes is provided in Appendix G (page 255) of the Risk Management Guide.

Section	Topic	Products
D Risk & Fraud	**Rule Weighting**	CPI MPI Lite

Main Document Reference	Risk Manager Guide, Chapter 8 Page 128

Weights are numeric values you assign to rules. By assigning weights to rules, you can control the impact a rule has on determining if a transaction is fraudulent. For example, a rule with a weight of 500 has relatively greater significance than a rule with a weight of 50. In order for weights to have an effect on rule processing, you must create at least one rule that evaluates *the TotalScore*.

A FraudShield rule can have an assigned weight that ranges between -1000 and 1000. Positive weights are assigned to rules that indicate a transaction is possibly fraudulent, while negative weights are assigned to rules that indicate a transaction is less likely to be fraudulent. The default weight assigned to a rule when no weight has been specified is zero.

An easy and effective way to utilise weights is to create a rule that evaluates a transaction's accumulated score. If the transaction's score exceeds a specified threshold, the rule carries out an action e.g. accept, reject or review.

Fraud rule weighting allows you to tailor the **Risk Management** tool to your own fraud policy. This is done by specifying weights to rules that you wish to use, by assigning an action of "none". You then create a separate rule to evaluate the total score of the weighted rules and after the total weight has been calculated take action (e.g. accept, reject or review) according to the final weight total (TotalScore).

With the current strategy rules, you set the order in which you want the rules to trigger, for example, You might want the rule to check for a certain name 'Jones' and set the action to reject this means that it will reject all orders with the name of Jones whereas your requirement may need to be more specific in that you want to reject the order from a customer with the name of Jones who lives at a certain address or using a particular card number or email address.

Alternatively, weighting allows you to create 'Accept' rules for loyal repeat customers who you know are genuine and you don't want them to be penalised by other rules that you may have set.

The addition of weights to a rule is managed from the Fraudshield Rule Management page.

To access this:

1. After you have logged into the store, click **Risk Management** from the top four options.
2. Select **Rules** from the **Settings** menu on the left. The '**Where are my fraud rules?'** page is displayed. Select **Click Here to view my rules,** the standard set of strategy rules is displayed.

Example – How to create a rule with weights

Scenario

You wish to block any transactions that meet the following criteria:

	Weight
• with an email address of Jones@test.co.uk	+100
• block a customer with the billing name of Jones and/or	+50
• using card number 4111111111111111	+100

1. From the 'Strategy Detail' page select the rule 'BlockEmailAddress'. The **My Rule Editor** page is displayed.
2. Assign a numerical weight e.g. 100 to the rule.
3. Set the **Action** and **Action On Missing Value** field to **None.**
4. Create a Merchant and Consumer Message as appropriate.
5. If you wish to receive an additional email advising that this rule has been triggered, enter an email address in **Send notification email to** field.
6. If you are happy with the details you have entered, select **Active Rule** at the top of the page and then press **Save** at the bottom of the page. The rule will now be active.

You now need to add the blocked email address to the **Lists**.

7. From the **Fraudshield Risk Management** page select **Lists** from the **Settings** menu on the left. The '**Risk Management' list** page is displayed.
8. From the **'I would like to'** section select **Add New List Values** (this is the default).
9. From the **'To the following list'** field select **'BlockEmailAddress'** and select **Next.**
10. In the **List Values** field add the email address to be blocked then select **Add your value to the list.**
11. Then **Save the changes to your list.**

Repeat step 1 to 11 for rule 'BlockBillingName' and rule 'BlockCardNumber'. Remember to allocate a different numerical weight for each one depending on how high you believe it to be indicative of fraud e.g. you might deem that blocking the card number is a higher weight than blocking the billing name.

You then need to create a rule that evaluates a transaction's accumulated score. If the transaction's score exceeds a specified threshold, the rule carries out an action e.g. accept, reject or review.

All new strategy rules are created from the Fraudshield Rule Management page. To access this:

1. From the '**Strategy Detail'** page scroll down to the bottom and press **Add.** A **New Rule** page will be displayed with a blank template fraud rule.
2. On the **New Rule** page enter the **Rule Name.** For this example enter "Weight score".
3. Select the **Process Phase** of **Pre-Process** as we wish the transaction to be checked before ePDQ obtains authorisation.
4. Select the **Attribute** of **Order Form Lists and TotalScore.**
5. Select the **Operator** of = **(Equal to or IN).**
6. Enter the value of the total score you wish to check, for example 200 into the **Value** field.
7. Click the **Add to Expression** button. The expression you have just built will be entered into the expression box.
8. Set the **Action** to **Reject**. This will mean that if the sum of the rule weighting exceeds the score you entered the transaction will be flagged as potentially fraudulent and will be rejected.
9. Set the **Action On Missing Value** to **None**.
10. Create a Merchant and Consumer Message as appropriate
11. If you wish to receive an additional email advising that this rule has been triggered, enter an email address in **Send notification email to** field.
12. If you are happy with the details you have entered, select **Active Rule** at the top of the page and then press **Save** at the bottom of the page. The rule will now be active.

TIP! It is recommended that any weighted rules come before any rules with Accept or Reject actions otherwise weighted rules will not be processed if those rules with an action evaluate to TRUE.

Section	Topic	Products
D Risk & Fraud	**Normalisation**	CPI MPI Lite

Main Document Reference	Risk Manager Guide, Chapter 7 Page 95

Address normalisation is a technique that can be used to improve street address matching during rule processing. Normalisation enables FraudShield to compensate for alternate spellings and misspellings of the same street address. (One fraud technique, for example, involves deliberately misspelling a BillTo address or a ShipTo address in order to disguise multiple orders from the same address or delivered to the same address.)

Scenario

You wish to reject all orders received from "1 the high street, NN47SG". By adding a normalised address rule, it will check for different combinations of that address such as:

1 High Street, nn47sg
1 High St, NN47SG
1 High str# NN47SG
1 Hgh Street, NN47SG
1 Hgh Str, NN47SG

All five examples are variations of the same address. Differences in spelling, punctuation, and capitalisation, however, can outsmart many address-matching routines. As a result, addresses which contain slight irregularities often fail to match properly.

FraudShield's address normalisation algorithm is more robust. FraudShield's address normalisation capabilities allow it to ignore the variations in the list above and return a match. This is because FraudShield's address normalisation algorithm creates a sophisticated representation of each address and postal code, and uses this representation to make comparisons. In the case of the five addresses listed above, all five would match because all five break down to the same normalised representation.

Example – How to create a normalised rule

All new normalised strategy rules are created from the Fraudshield Rule Management page. To access this:

1. After you have logged into the store, click **Risk Management** from the top four options.
2. Select **Rules** from the **Settings** menu on the left. The '**Where are my fraud rules?'** page is displayed. The standard set of strategy rules are displayed.

3. From the **'Where are my fraud rules?'** page, scroll down to the bottom and select **'Click here to view My Rules'**. The standard set of strategy rules are displayed.
4. Scroll down to the bottom of the page and press **Add**. A New Rule page will be displayed with a blank template fraud rule.
5. On the **New Rule** page enter the **Rule Name.** For this example enter "Normalised Address check".
6. Select the **Process Phase** of **Pre-Process** as we wish the transaction to be checked before ePDQ obtains authorisation.
7. Select the **Attribute** of **Built in Function and BillToNormalizedAddress**
8. Select the **Operator** of = **(Equal to or IN).**
9. Click the **Add to Expression** button.
10. Now select the **Attribute** of **Standard Lists** and **BlockBillToAddressNorm**
11. Click the **Add to Expression** button. The expression you have just built will be entered into the expression box.
12. Set the **Action.** For this example, you would set to Reject.
13. Set the **Action On Missing Value** to **None**.
14. Create a Merchant and Consumer Message as appropriate
15. If you wish to receive an additional email advising that this rule has been triggered, enter an email address in **Send notification email to** field.
16. If you are happy with the details you have entered, select **Active Rule** at the top of the page and then press **Save** at the bottom of the page. The rule will now be active.

You now need to add the blocked address to the **Lists**.

17. From the **Fraudshield Risk Management** page select **Lists** from the **Settings** menu on the left. The **'Risk Management Lists?'** page is displayed.
18. From the **'I would like to'** section select **Add New List Values** (this is the default).
19. From the **'To the following list'** field select **'BlockBillToAddressNorm'** and select **Next.**
20. In the **Street** field add the street address to be blocked then in the **Postal code** field add the Postal code to be blocked then **Add your value to the list.** The values will then be shown in the list value.
21. Then **Save the changes to your list**

Barclaycard Payment Acceptance is a trading name of Barclay Bank PLC.. Barclays Bank PLC is authorised and regulated by the Financial Services Authority. Registered in England. Registered No: 1026167. Registered Office: 1 Churchill Place, London E14 5HP